

1 **In the Claims**

2 Claims 1, 5, 11, 15, 21, 25 and 26 are currently amended.

3 Claims 3, 4, 13, 14, 23 and 24 are canceled without prejudice.

4 Claims 1, 2, 5-12, 15-22, 25 and 26 remain in the application for
5 consideration and are listed as follows:

6
7 1. (Currently Amended) A method for use in a computer capable of
8 supporting multiple authentication mechanisms, the method comprising:
9 generating at least one indicator that identifies a user, and is associated with
10 and identifies at least one authentication mechanism that has been used to
11 authenticate the user, wherein generating the indicator further includes identifying
12 within the indicator at least one characteristic associated with the authentication
13 mechanism, wherein the at least one characteristic associated with the
14 authentication mechanism includes a measure of strength of the authentication
15 mechanism; and

16 controlling the user's access to at least one resource based on the indicator.

17
18 2. (Original) The method as recited in Claim 1, wherein generating the
19 indicator further includes receiving inputs, providing the inputs to the
20 authentication mechanism, and causing the authentication mechanism to generate
21 at least one security identifier (SID) that identifies the authentication mechanism.

22
23 3. (Canceled).

24
25 4. (Canceled).

1
2 5. (Currently Amended) The method as recited in Claim [[4]] 1,
3 wherein the measure of strength of the authentication mechanism identifies a
4 length of an encryption key employed by the authentication mechanism.
5

6 6. (Original) The method as recited in Claim 1, wherein controlling
7 access to the resource based on the indicator further includes comparing the
8 indicator to at least one access control list having at least one access control entry
9 therein.
10

11 7. (Original) The method as recited in Claim 6, wherein if the access
12 control entry operatively specifies that the at least one authentication mechanism
13 is permitted to access the resource, then access to the at least one resource is
14 allowed to proceed.
15

16 8. (Original) The method as recited in Claim 6, wherein if the access
17 control entry operatively specifies that the at least one authentication mechanism
18 is not permitted to access the resource, then access to the at least one resource is
19 not allowed to proceed.
20

21 9. (Original) The method as recited in Claim 6, wherein if the access
22 control entry does not operatively specify that the at least one authentication
23 mechanism is permitted to access the resource, then access to the at least one
24 resource is not allowed to proceed.
25

1 10. (Original) The method as recited in Claim 1, wherein the indicator
2 includes a security token.

3
4 11. (Currently Amended) A computer-readable medium for use in a
5 device capable of supporting multiple authentication mechanisms, the computer-
6 readable medium having computer-executable instructions for performing acts
7 comprising:

8 producing at least one indicator that identifies a user, and uniquely
9 identifies at least one authentication mechanism supported by the device that has
10 been used to authenticate the user, wherein producing the indicator further
11 includes identifying within the indicator at least one characteristic of the
12 authentication mechanism, wherein the at least one characteristic of the
13 authentication mechanism includes a strength characteristic of the authentication
14 mechanism; and

15 causing the device to selectively control the user's access to at least one
16 resource operatively coupled to the device based at least in part on the indicator.

17
18 12. (Original) The computer-readable medium as recited in Claim 11,
19 wherein producing the indicator further includes receiving inputs, providing the
20 inputs to the authentication mechanism, and causing the authentication mechanism
21 to generate at least one security identifier (SID) that identifies the authentication
22 mechanism, in response thereto.

23
24 13. (Canceled).

1 14. (Canceled).

2
3 15. (Currently Amended) The computer-readable medium as recited in
4 Claim [[14]] 12, wherein the strength characteristic identifies a length of an
5 encryption key employed by the authentication mechanism.

6
7 16. (Original) The computer-readable medium as recited in Claim 11,
8 wherein causing the device to selectively control access to the at least one resource
9 based on the indicator further includes causing the device to compare the indicator
10 to control data .

11
12 17. (Original) The computer-readable medium as recited in Claim 16,
13 wherein if the control data specifies that the authentication mechanism is
14 permitted to access the resource, to which subsequent access to the resource is
15 allowed.

16
17 18. (Original) The computer-readable medium as recited in Claim 16,
18 wherein if the control data operatively specifies that the authentication mechanism
19 is not permitted to access the resource, to which subsequent access to the resource
20 is prohibited.

21
22 19. (Original) The computer-readable medium as recited in Claim 16,
23 wherein if the control data does not operatively specify that the authentication
24 mechanism is permitted to access the resource, to which subsequent access to the
25 resource is prohibited.

1
2 20. (Original) The computer-readable medium as recited in Claim 10,
3 wherein the indicator includes a security token.
4

5 21. (Currently Amended) An apparatus comprising:
6 at least one authentication mechanism configured to generate at least one
7 indicator that identifies a user, and identifies the authentication mechanism that
8 has been used to authenticate the user, wherein the indicator further includes at
9 least one identifying characteristic associated with the authentication mechanism,
10 wherein the at least one identifying characteristic associated with the
11 authentication mechanism indicates a measure of strength of the authentication
12 mechanism;

13 an access control list;
14 at least one access controlled resource; and
15 logic operatively configured to compare the indicator with the access
16 control list and selectively control the user's access to the resource based on the
17 indicator .
18

19 22. (Original) The apparatus as recited in Claim 21, wherein the
20 authentication mechanism is further configured to receive user inputs and generate
21 at least one security identifier (SID) that identifies the authentication mechanism
22 based on the user inputs.
23

24 23. (Canceled).
25

1 24. (Canceled).

2
3 25. (Currently Amended) The apparatus as recited in Claim ~~[[24]]~~ 21,
4 wherein the measure of strength of the authentication mechanism identifies a
5 length of an encryption key employed by the authentication mechanism.

6
7 26. (Currently Amended) The apparatus as recited in Claim ~~[[23]]~~ 21,
8 wherein the indicator includes a security token.